REMARKS

Claims 23, 25-33 and 35-41 are pending. Claims 23, 25-27, 30, 33 and 39 were amended to address the rejection under 35 U.S.C. § 112, first paragraph. Claims 24 and 34 were canceled.

Request for Interview Prior to Formal Action on Amendment

Applicant requests an interview prior to formal action on this amendment. An "Applicant Initiated Interview Request Form" accompanies this response. Please contact Applicants' undersigned representative to schedule the interview. Applicant's previous request for an interview was denied on the grounds that an interview was already conducted and that any subsequent interview conducted is at the discretion of the Examiner. In response, Applicant asserts that the grounds of rejection were substantially changed from rejections based on Messmer to rejections based on Emigh, and thus completely new issues need to be discussed regarding the basis for the Emigh-based rejections. The Examiner's explanations discussed in detail below for continuing to rely upon Emigh further highlight the need to hold another interview to discuss how the claimed invention differs from Emigh.

35 U.S.C. § 112, first paragraph, rejection

1. Claims 24 and 34

The rejection of these claims is rendered moot by the cancellation of these claims.

2. Claim 25

The rejection of this claim is rendered moot by the cancellation of the second clause of this claim. The first clause of claim 25 mirrors the exact language provided on page 8, line 31 through page 9, line 6 of the specification, which reads as follows (underlining added for emphasis):

> Although information preferably flows both ways between master system 60 and security subsystem 50 in this embodiment, the master system in this embodiment does not take direction from the subsystem.

Accordingly, withdrawal of this rejection as it pertains to amended claim 25 is respectfully requested.

Claims 26 and 27

Claim 26 was amended to refer to a second secure link, which in one embodiment of the present invention constitutes secure links 55 shown in Fig. 2. Page 9, lines 17-19 of the specification, which reads as follows, describes the function of the secure links 55:

> Additionally, if the link 54 between master system 60 and security subsystem 50 is severed or compromised, instructions may be routable instead through secure links 55.

Amended claim 26 is clearly supported by at least Fig. 2 and the above-highlighted text. Accordingly, withdrawal of this rejection as it pertains to amended claim 26 and unamended claim 27 (which is dependent upon claim 26 and which was rejected solely due to this dependency) is respectfully requested.

Prior Art Rejections

Claims 23, 28-29, 33 and 40-41 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Emigh. This rejection is respectfully traversed.

Applicant incorporates by reference the arguments presented in the previous Amendment filed August 12, 2005. See pages 9-12 of the previous Amendment.

On page 6 of the Final Rejection, the Examiner responded to certain arguments presented in the previous Amendment.

1. Emigh does not disclose or suggest a master system which monitors the integrity of a security subsystem as recited in claims 23 and 33

The Examiner has now clarified on page 6 of the Final Rejection that the claimed security subsystem is met by the NetRanger sensor. The Examiner previously identified the NSOC as being equivalent to the claimed master system.

Emigh has no disclosure or suggestion that the NSOC (the alleged "master system") monitors the integrity of the NetRanger sensor (the alleged "security subsystem"). To support this position, the Examiner states on page 6 of the Final Rejection that Emigh teaches that IBM's NSOC located in Boulder conducts monthly testing of network devices like web servers for vulnerability. This statement does not provide any support for the Examiner's assertion that Emigh meets this claim limitation.

Vulnerability is a completely different concept than integrity, and thus testing for vulnerability is not the same as, or equivalent to, testing for integrity. Vulnerability relates to the susceptibility of a device to attack, whereas integrity relates to whether the device is in a state of being unimpaired. A device can be vulnerable but still have its integrity intact, and vice-versa. See the attached Appendix which includes dictionary definitions and Google web-located definitions of vulnerability and integrity as further evidence that these words mean completely different things, and that testing for vulnerability does not mean that one has tested for integrity.

Furthermore, even if it can be somehow justified that testing for vulnerability is the same as testing for integrity, Emigh never even states that the NSOC tests the NetRanger sensor for vulnerability. Emigh merely states that network devices like web servers are tested for vulnerability.

In sum, the statement highlighted by the Examiner in Emigh is clearly deficient in meeting clause (b) of independent claims 23 and 33.

2. Emigh does not disclose or suggest a security subsystem that monitors activities of devices on a network as recited in claim 23

The Examiner has responded to this argument by asserting on page 6 of the Final Rejection that the NetRanger sensor monitors devices because Emigh states that the NetRanger

sensor is placed on a corporate network such as Internet and intranet connections. This statement does not provide any support for the Examiner's assertion that Emigh meets this claim limitation.

NetRanger is indeed placed on a corporate network such as Internet and intranet connections, but that is because NetRanger has the specific purpose of detecting and analyzing IP network traffic (i.e., traffic among and between devices on the network) and Internet or intranet connections is one location where such network traffic can be monitored. This does not mean that NetRanger monitors activities of devices on the corporate network. Again, the Examiner has equated two disparate functions, each of which can be performed independent of the other, namely detecting and analyzing IP network traffic with monitoring activities of devices on a network.

Consider an attack on a network device that is made by a path other than the network itself, such as by direct keyboard entry into the device, or by a non-network related input port of the device. Since NetRanger detects and analyzes only IP network traffic, and does not monitor activities of devices on a network, such attacks may go undetected, particularly if the attack does not cause unusual IP network traffic to occur among and between the devices on the network.

3. Patentability of claims 23 and 33 over Emigh

For at least the reasons discussed above, Emigh fails to disclose or suggest the claimed combination of a security subsystem and a master system, and at least the following underlined limitations:

> 23. A security system for a computer network, the network having a plurality of devices connected thereto, the security system comprising:
> (a) a security subsystem connected to at least some of the devices in the network, the security subsystem configured to monitor activities of the at least some devices on the network and detect attacks on the at least some devices;
> (b) a master system which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem; and
> (c) a first communication medium secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks through the first communication medium secure link.

33. A security system for a computer network, the network having a plurality of devices connected thereto, at least some of the devices having security-related functions, the security system comprising:
(a) a security subsystem associated with at least some of the devices in the network which tests the integrity of the security-related functions;
(b) a master system which monitors the integrity of the security subsystem and receives and stores results of the integrity testing of the devices having security-related functions; and
(c) a communication medium secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the results of the integrity testing of the devices having security-related functions through the first communication medium secure link.

In view of the above remarks, claims 23 and 33 are believed to be patentable over Emigh.

4. Patentability of dependent claims 25-32 and 35-41

The dependent claims are believed to be patentable over the applied references for at least the reason that they are dependent upon allowable base claims and because they recite additional patentable elements and steps.

Conclusion

Insofar as the Examiner's rejections were fully addressed, the instant application is in condition for allowance. Issuance of a Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectfully submitted,

MICHAEL HRABIK et al.

December 15, 2005 By: Anna Vishev

ANNA VISHEV
Registration No. 45,018
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022
Telephone: (212) 756-2000
Direct Dial: (212) 756-2167
Facsimile: (212) 593-5955
E-Mail: anna.vishev@srz.com

Enclosure (Appendix, 10 pages)